Podpis elektroniczny

Kryptografia asymetryczna obsługiwana jest poprzez wbudowane w system funkcje do podpisywania i szyfrowania dokumentów. Certyfikaty pracowników można zaimportować poprzez panel kont pracowników (zakładka Certyfikaty).

Po włączeniu opcji pozwalającej używać funkcji kryptograficznych w pliku config.inc:

```
define('USE_OPENSSL', TRUE);
```

można podpisywać i szyfrować notatki służbowe oraz załączniki do dokumentów.

Aby zapobiec sytuacjom w którym firma traci dostęp do zaszyfrowanych przez pracowników danych eDokumenty (na skutek zapomnienia hasła, odejścia pracownika bez podania hasła, wypadków itp.) wprowadzają funkcjonalność sejfu, w którym przechowywane są zaszyfrowane klucze pracowników.

Klucze prywatne szyfrowane są kluczem publicznym sejfu, przez co mogą być odszyfrowane wyłącznie poprzez podanie hasła do samego klucza lub hasła do klucza prywatnego sejfu.

Klucz sejfu można dodać poprzez prosty skrypt powłoki:

```
#!/bin/bash

if [ "$1" == "" ]; then
   echo "Usage: $0 <dbname>"
   exit 1
fi

CERTIFICATE=''
PUBLICKEY=''
PRIVATEKEY=''

DBNAME=$1
psql $DBNAME -c "INSERT INTO certificates (cert__, pu_key, pr_key, issafe) values ('$CERTIFICATE', '$PUBLICKEY', '$PRIVATE
```

Ewentualnie poprzez wykonanie zapytania na bazie danych w PgAdmin, wstawiając w odpowiednie pola właściwe dane.

UWAGA!

Klucz prywatny sejfu również musi mieć założone hasło!!! Klucz sejfu powinien zostać dostarczony z hasłem przez kierownika jednostki (np. Prezesa/Dyrektora/Właściciela). Ewentualnie hasło powinno zostać podane podczas tworzenia klucza - należy wezwać kierownika jednostki do zdefiniowania hasła i zdeponować go w opisanej kopercie w sejfie fizycznym.